



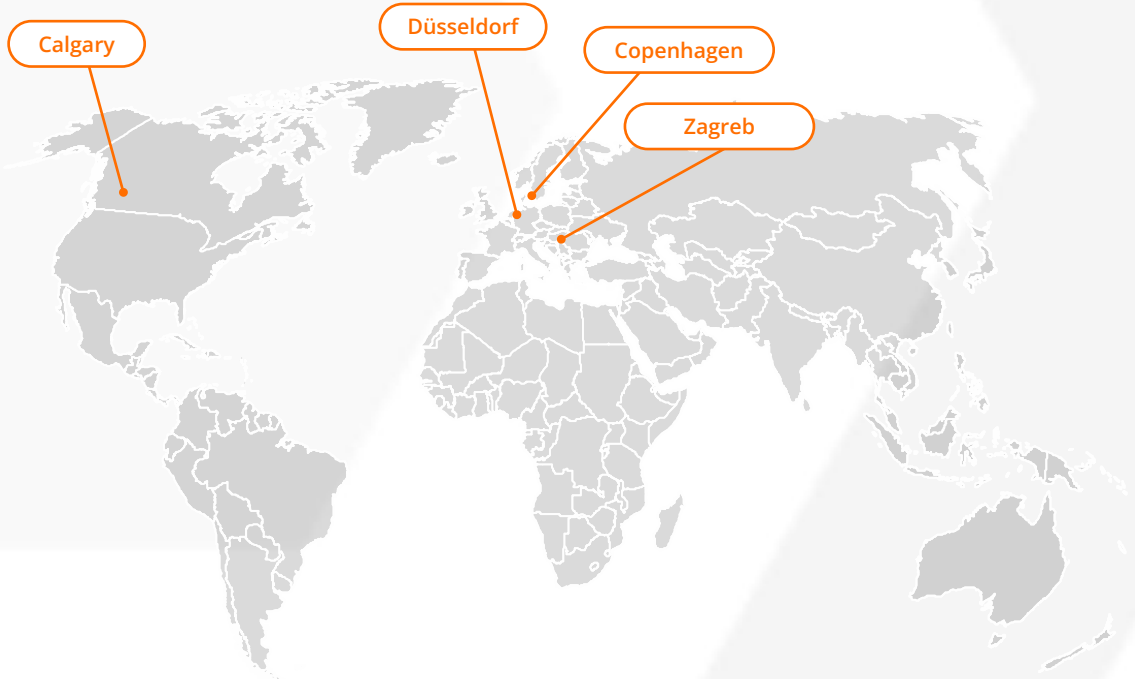
Introducing Data & More

Protecting digital privacy and minimizing the risk, cost, and liability of processing unstructured data by automatically removing Privacy Data from Mail, OneDrive, SharePoint, and File Shares.

Data More Denmark: +45 4290 1070 - Flaesketoerret 68, 1711 Copenhagen V, Denmark
Data More Germany: +49 151 59422362 - Am Steinebrück 29, 40589 Düsseldorf, Germany
Data More Canada: +1.587.966.9070 - 500 - 4th Avenue SW, Calgary, Alberta, Canada



About Data & More



Protecting digital privacy and minimizing the risk, cost, and liability of processing unstructured data.

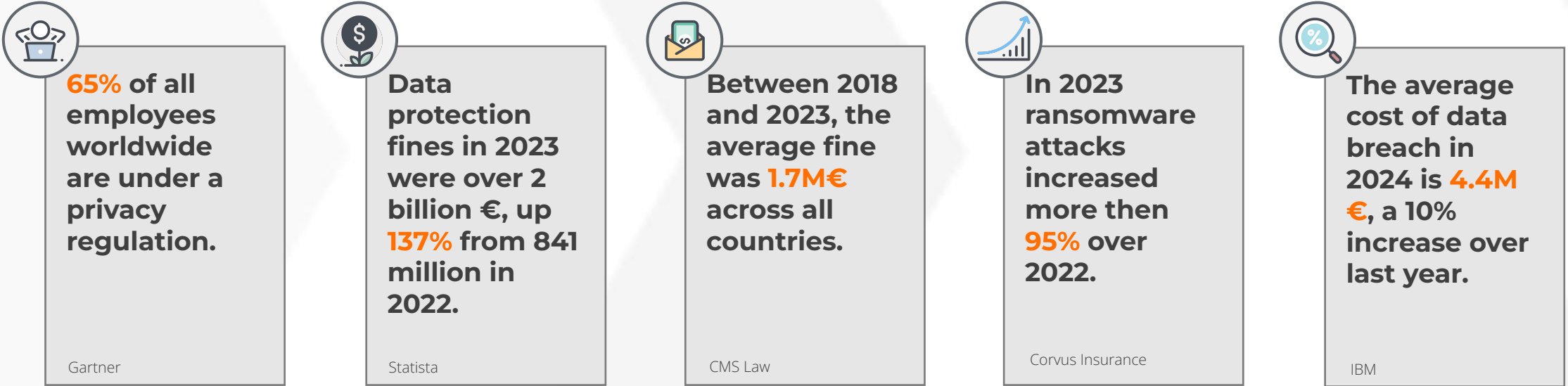
We help organizations delete data that has become illegal to keep as a result of e.g. Privacy regulations - or that has had a data breach, and therefore must inform the affected data subjects.

+ 150,000 end users
+3,000,000,000 protected datasets





The risk of doing nothing | Data Privacy Risk Premium



RISK OF FINES | RISK OF REPUTATION | RISK OF EXPLOITATION



Data Privacy Risk Premium



Understanding the Problem

All organisations have the same unstructured data & compliance challenges

- Large amounts of unstructured data - an average user has **55,000** data sets.
- Unstructured data is growing at a rate of **20-25%** each year (IDC).
- **1-2%** of all unstructured data contains "illegal" personal sensitive information.
- **0.2%** of unstructured data contains security information stored in plain-text.
- Permissions and data sharing are difficult to administer, resulting in lots of over-sharing.
- Unstructured data often has no identified owner.
- It's easier to purchase more storage than to effectively clean up old data.

What it Means

1. Data clean up isn't being done >>> increased risk and regulatory fines.
2. Many organizations are spending a lot of money on information management programs >>> seeing very little change in their overall data security posture.
3. Often organizations are afraid of impacting business processes and user productivity >>> struggle with how to implement information management change.

Why Data Minimization



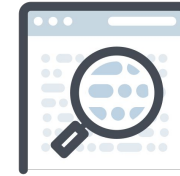
Data Compliance

When data is compliant there are **no regulatory fines** and is **no loss of reputation**.



Data Security

When data is compliant sensitive data is properly protected and plain-text credentials are removed, **significantly reducing the risk of a data breach**.



Data Breach

When data is compliant, the cost of a data breach is drastically reduced
Data & More also provides data subject



If you use Copilot or Purview, it enables compliance



Copilot

Data & More for Copilot enables organizations to **meet Copilot's data security and information management prerequisites**.

This means Copilot can be **implemented responsibly** and **without creating data breaches**.



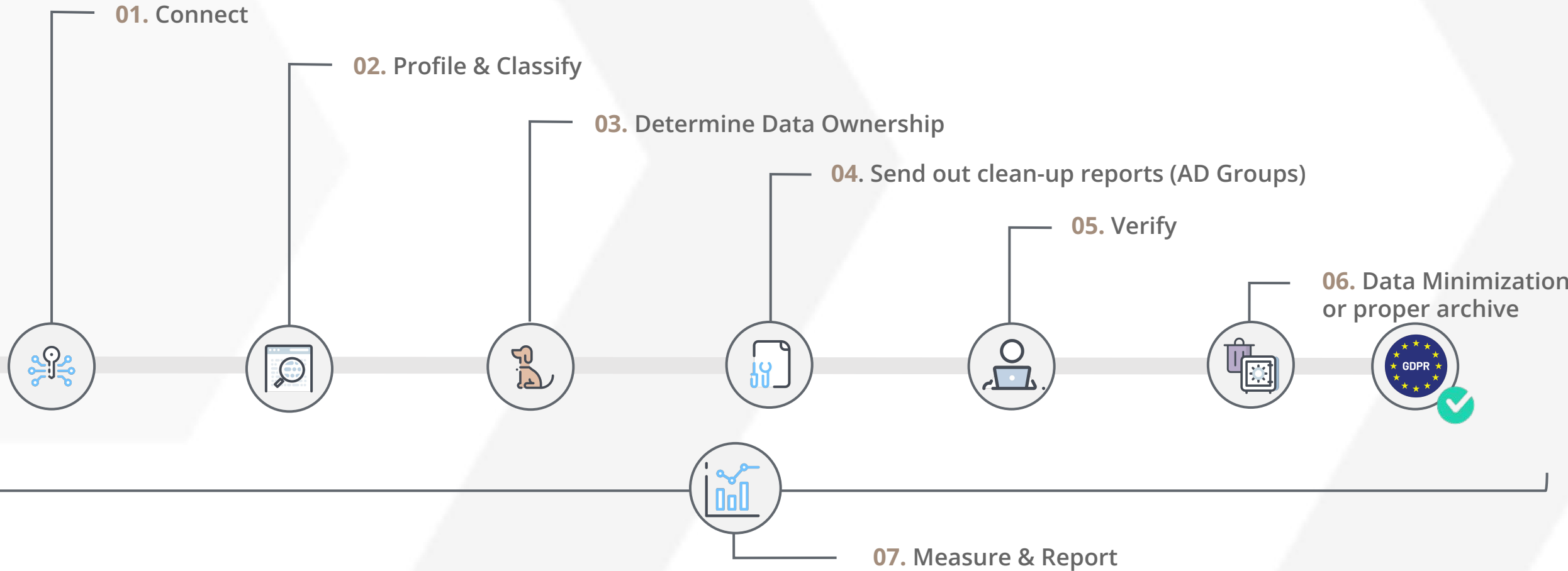
Purview

Data & More for Purview complements Microsoft's content classification, ensuring labels are set correctly so Purview policies are **protecting the right documents**.

It also provides visibility into any privacy data NOT protected by Purview so those **exceptions can be addressed**.

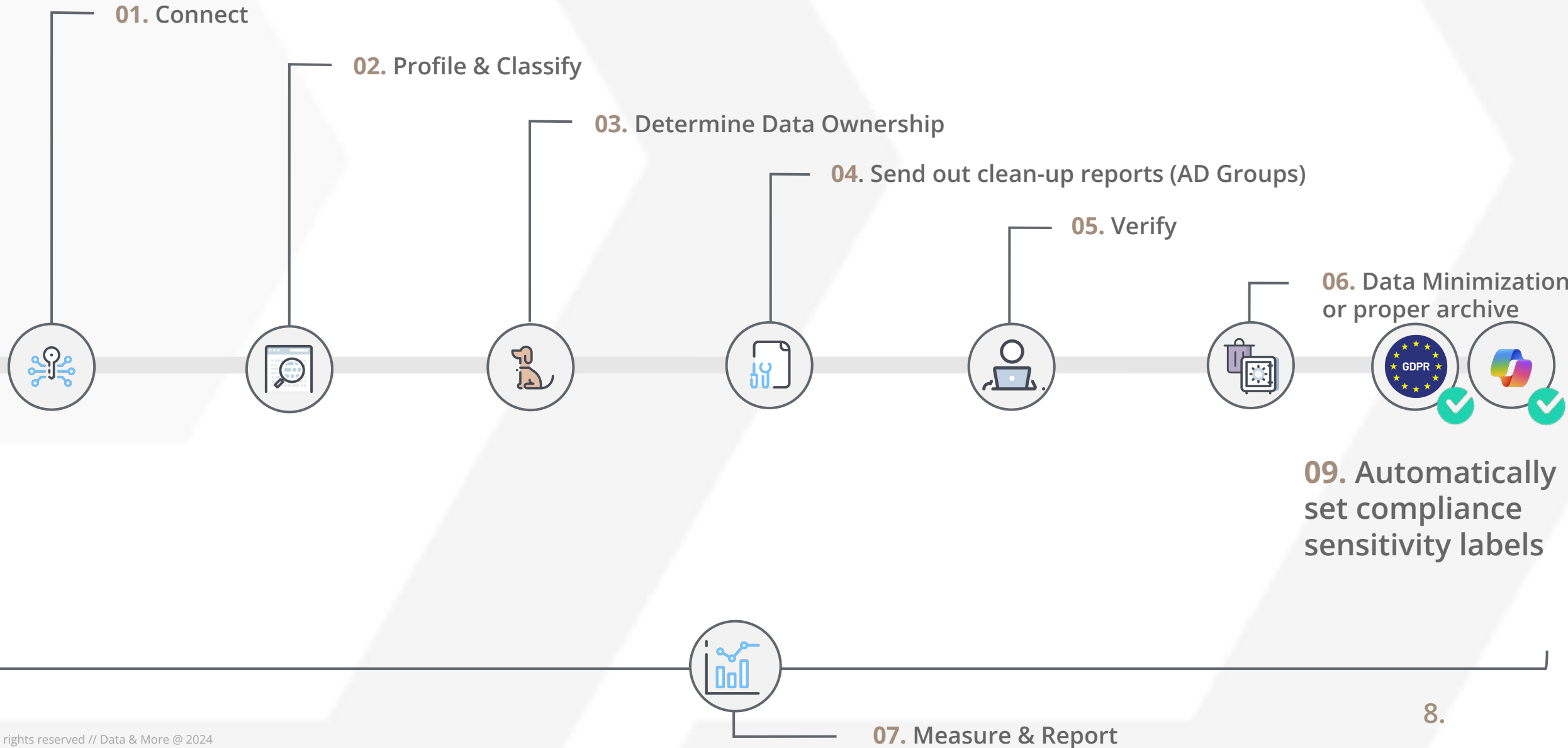


Data & More Data **Minimization**



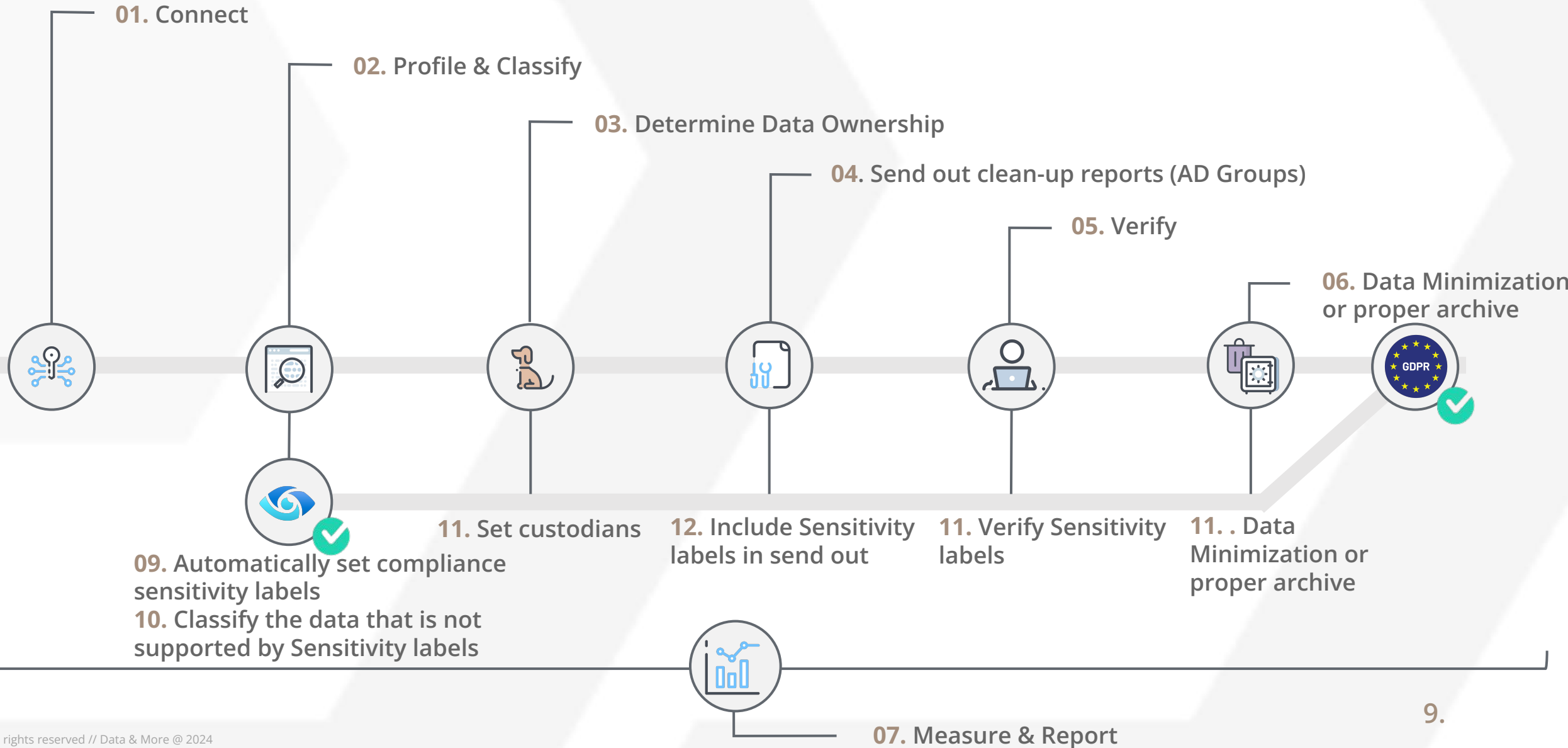


Data & More for Copilot



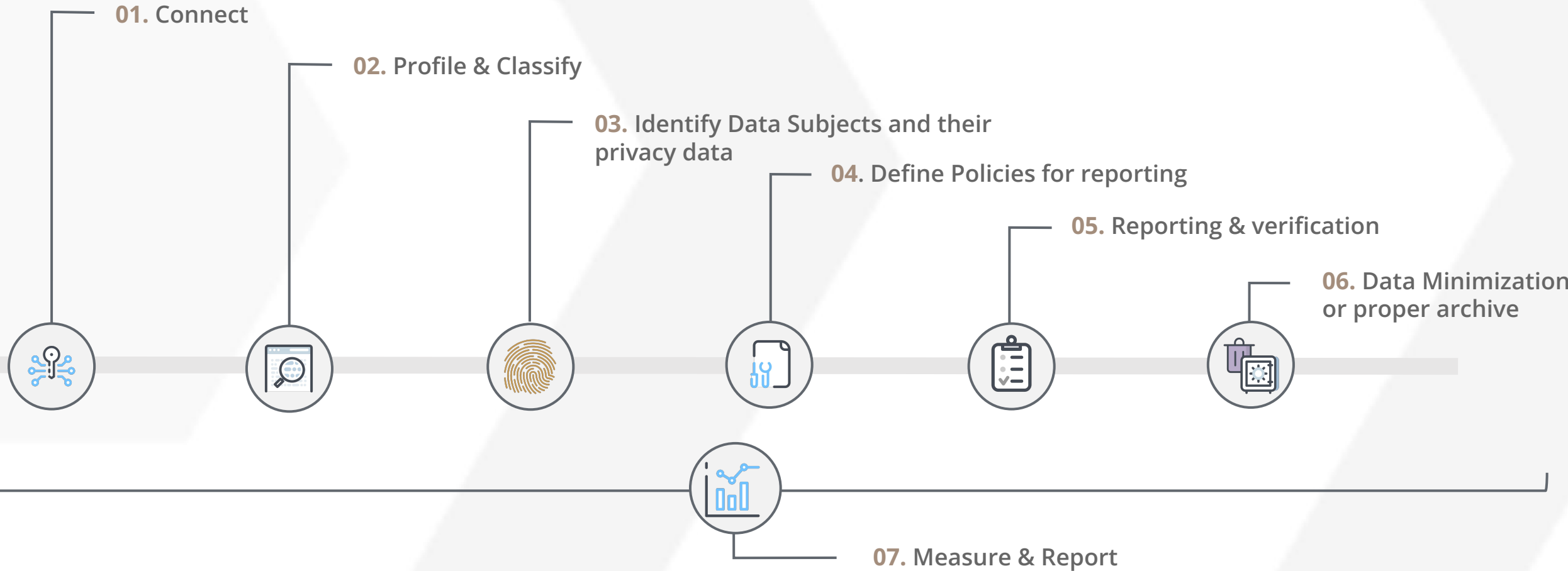


Data & More for Purview





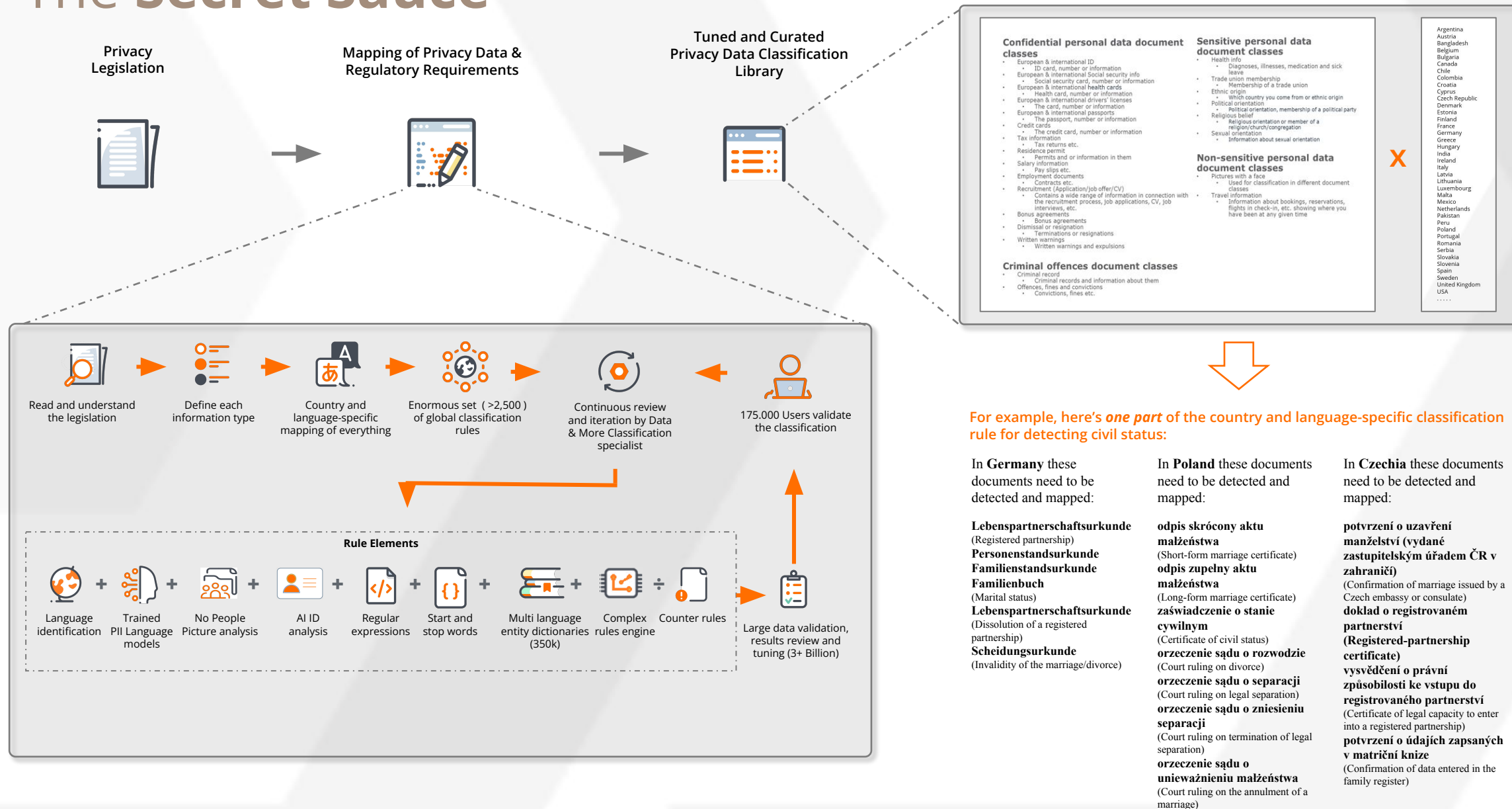
Data & More for **Data Breach** – Data subject analysis





The Secret Sauce

<https://support.dataandmore.com/en/knowledge/what-is-gdpr-data-classification>

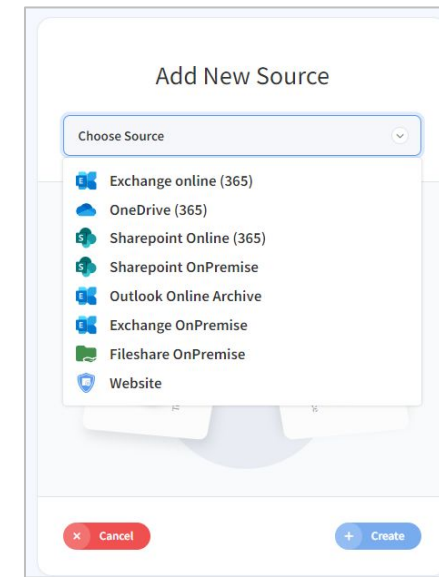
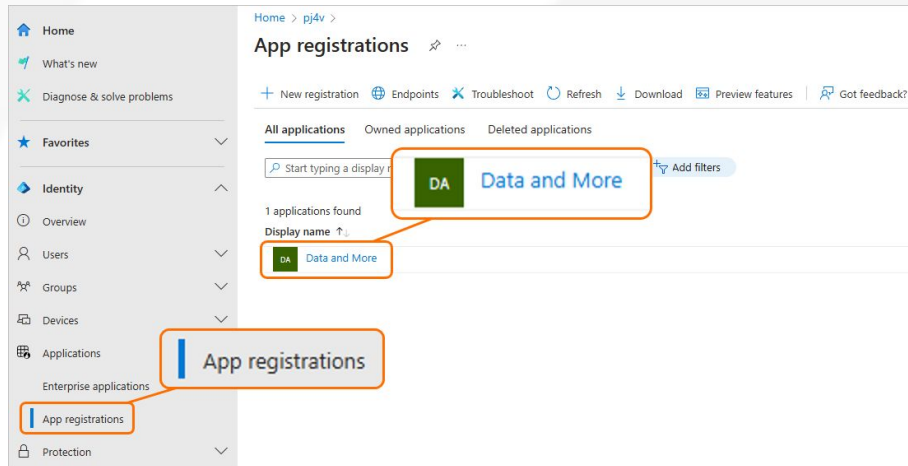
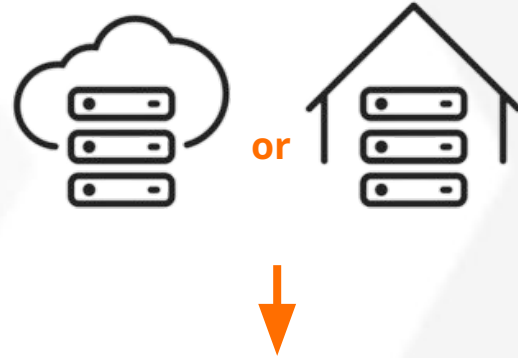




Solution Walkthrough



01. Setup infrastructure & Connecting Data Sources





02. Profile & Classify

See Article 6 of the Data Protection Regulation

Confidential personal data document classes

- European & international ID
 - ID card, number or information
- European & international Social security info
 - Social security card, number or information
- European & international health cards
 - Health card, number or information
- European & international drivers' licenses
 - The card, number or information
- European & international passports
 - The passport, number or information
- Credit cards
 - The credit card, number or information
- Tax information
 - Tax returns etc.
- Residence permit
 - Permits and or information in them
- Salary information
 - Pay slips etc.
- Employment documents
 - Contracts etc.
- Recruitment (Application/job offer/CV)
 - Contains a wide range of information in connection with the recruitment process, job applications, CV, job interviews, etc.
- Bonus agreements
 - Bonus agreements
- Dismissal or resignation
 - Terminations or resignations
- Written warnings
 - Written warnings and expulsions

Criminal offences document classes

- Criminal record
 - Criminal records and information about them
- Offences, fines and convictions
 - Convictions, fines etc.

See Article 9 of the Data Protection Regulation

Sensitive personal data document classes

- Health info
 - Diagnoses, illnesses, medication and sick leave
- Trade union membership
 - Membership of a trade union
- Ethnic origin
 - Which country you come from or ethnic origin
- Political orientation
 - Political orientation, membership of a political party
- Religious belief
 - Religious orientation or member of a religion/church/congregation
- Sexual orientation
 - Information about sexual orientation

Non-sensitive personal data document classes

- Pictures with a face
 - Used for classification in different document classes
- Travel information
 - Information about bookings, reservations, flights in check-in, etc. showing where you have been at any given time

See Article 6 of the Data Protection Regulation

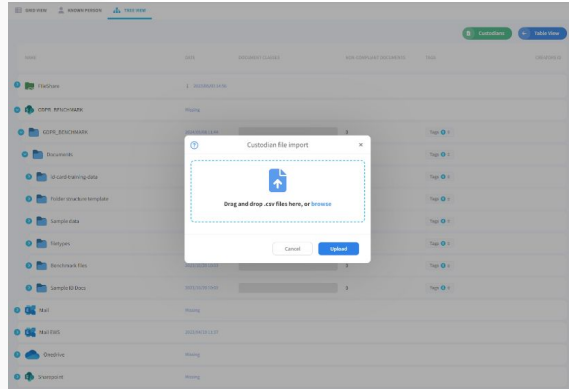
Information on criminal offences as referred to in Article 11(1) of Directive 91/ Articles 10 and 8 of the Data Protection Act



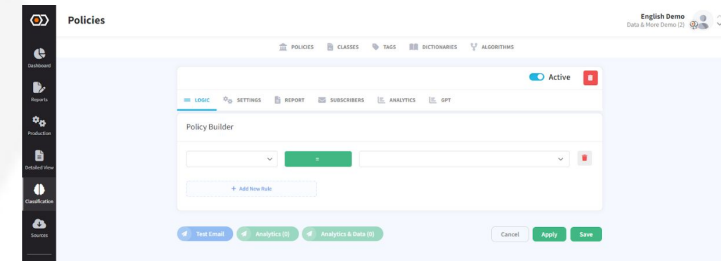


03. Determine Ownership (Custodian Mapping)

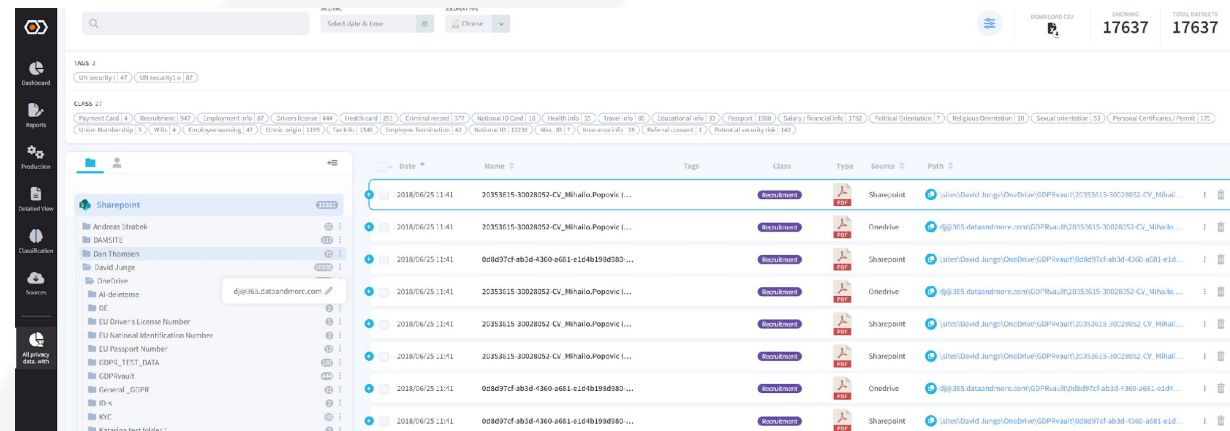
Bulk Custodian Mapping



Individual Custodian Reports

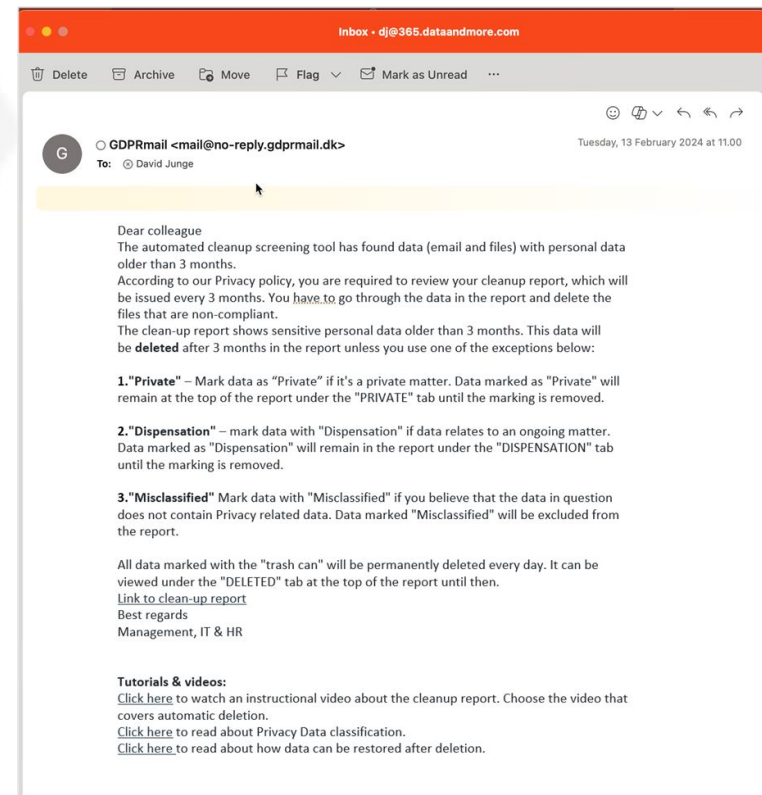
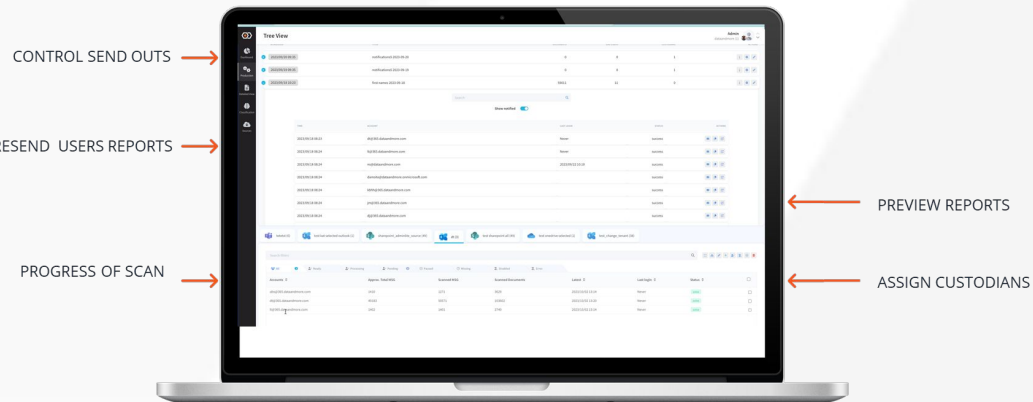


Custodian Mapping with Privacy Overview



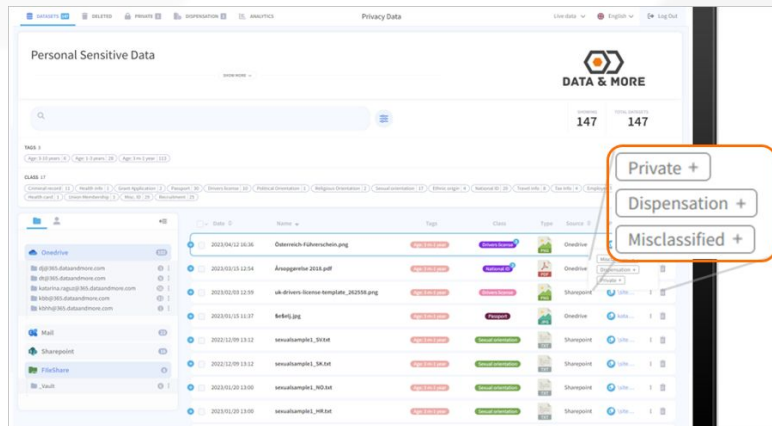
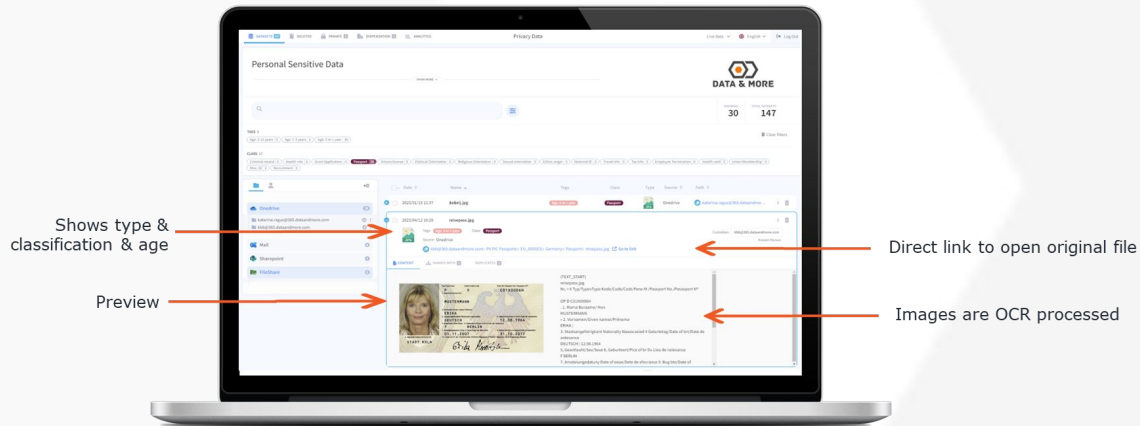


04. Configure & Send Cleanup Reports





05. User Review & Privacy Data Marking

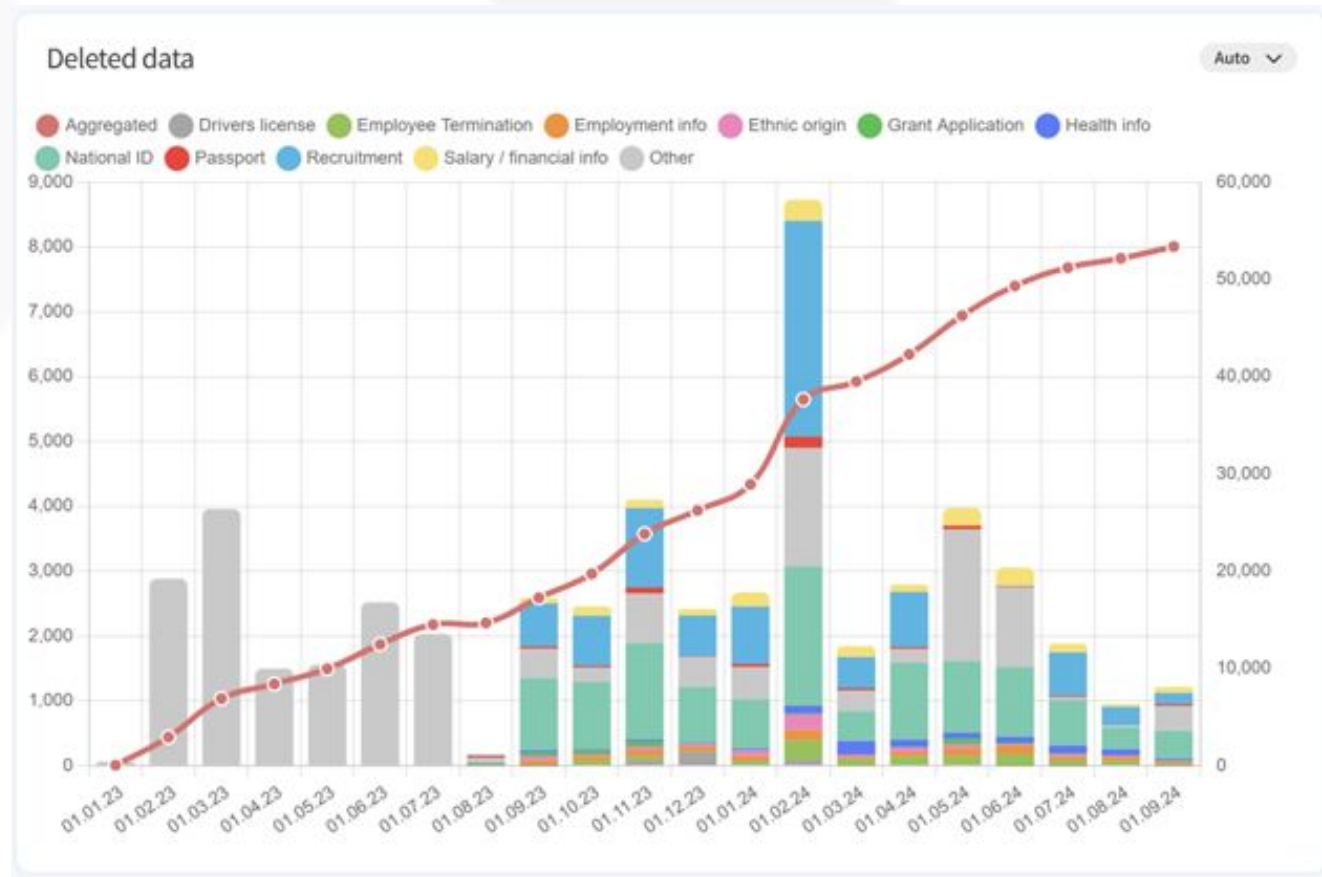


Workflow

1. Each employee receives a report containing only the personal sensitive data they are responsible for.
2. The employee can review individual items to see:
 - a. The age of each file,
 - b. Who each file is shared with,
 - c. Where there are duplicates,
 - d. What privacy data was found and how the item is classified.
3. The employee decides how each item is handled and marks each item from the options provided by the organization.



06. Privacy Data Cleanup (Delete & Archive)



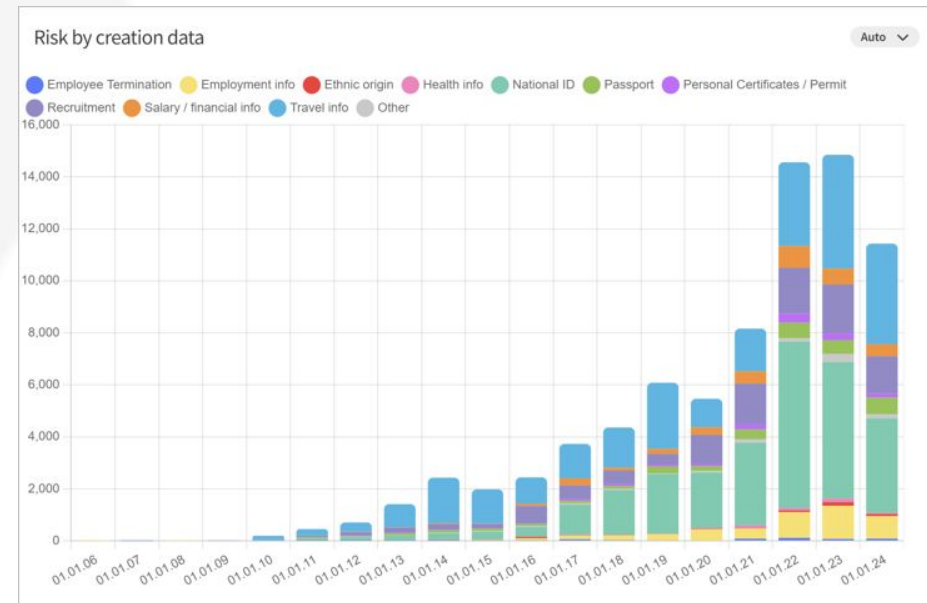


07. Measure & Report

Privacy Data by Type



Privacy Data by Age

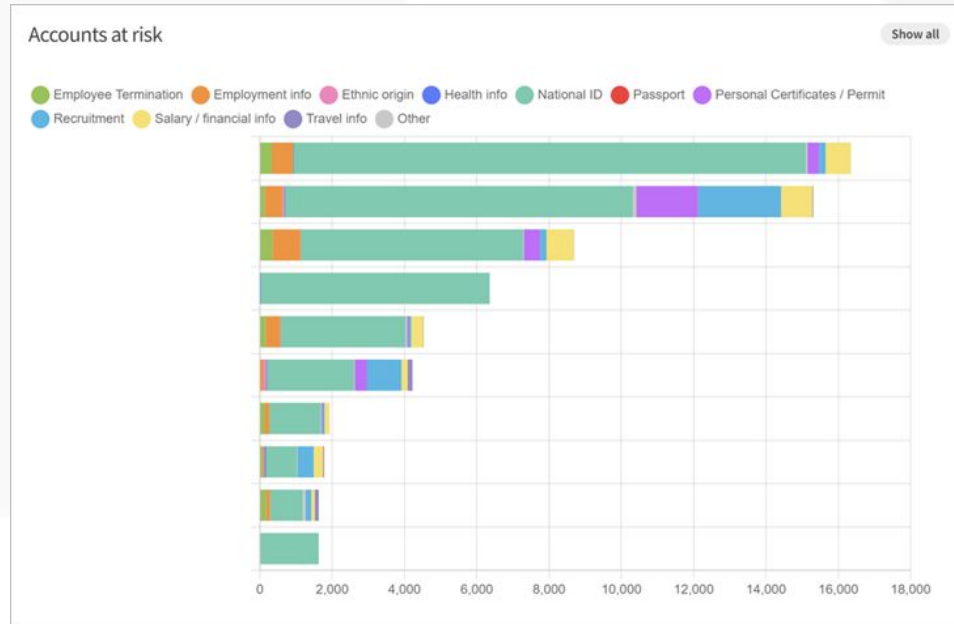




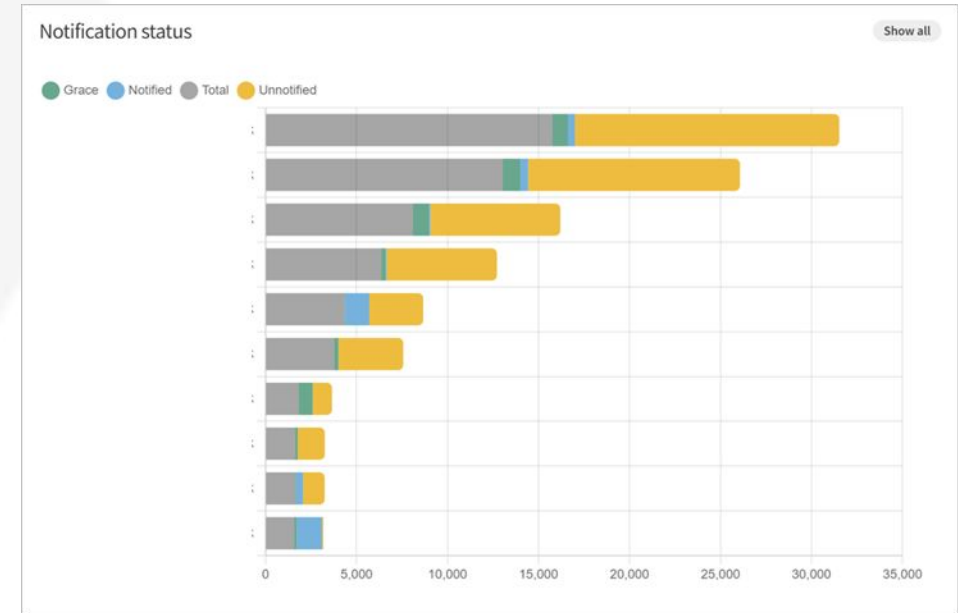
07. Measure & Report

(Continued)

Privacy Data by Type and Account



Privacy Data by Account and Status

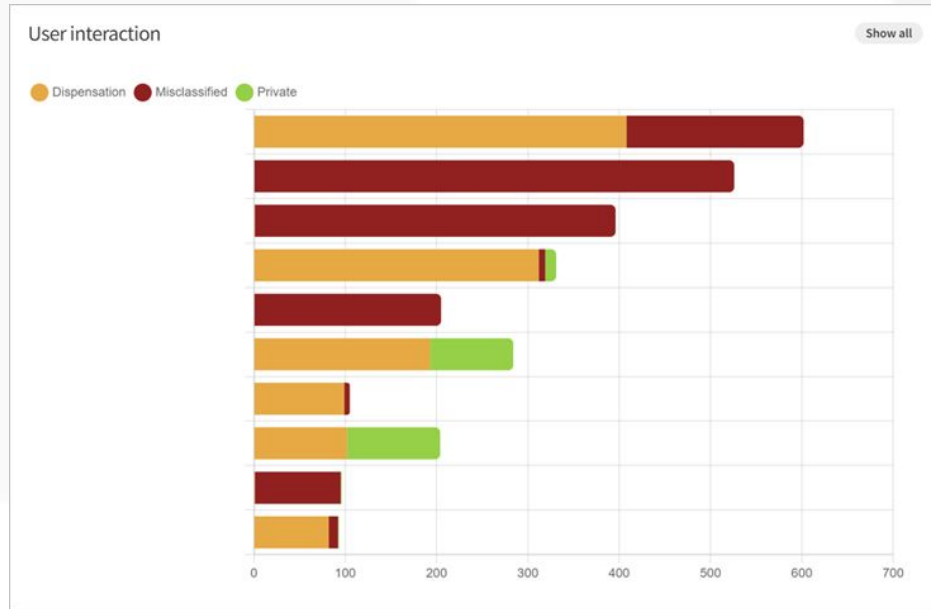




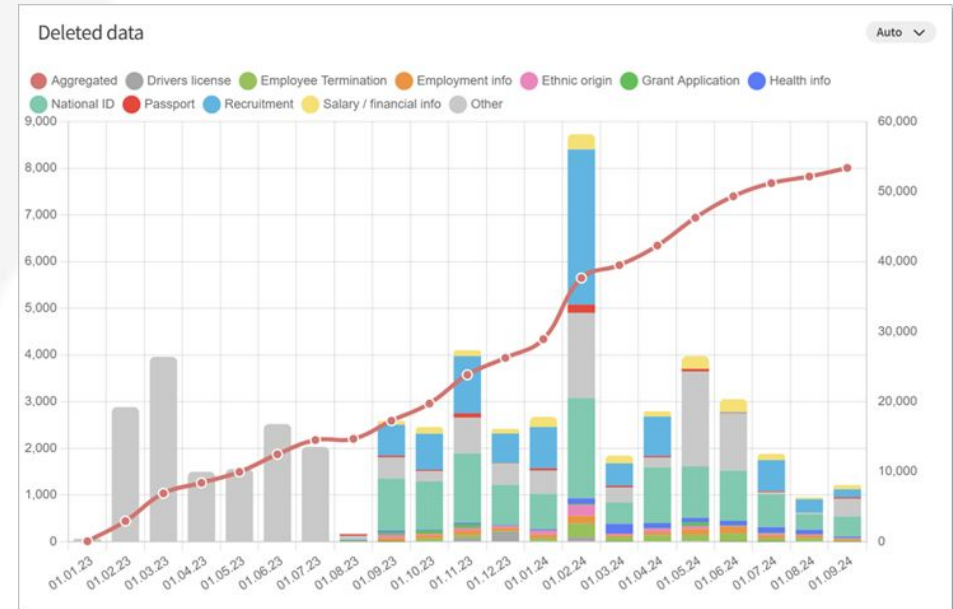
07. Measure & Report

(Continued
)

Document Marking Summary



Privacy Data Deletion Summary





Appendix A

PoC



Proof of Concept



Duration – approx. 1 month.

Only requires 3 x 45 min engagement

See description on our support site: [POC/Trial](#)



Appendix B

High Level Implementation plan

Implementation plan

Role: IT department
Effort: 1-2 day

IT Onboarding



Define:

- Which sources to scan
- Infrastructure to setup
 - On premise
 - SaaS
 - Cloud
- Setup infrastructure
- Connect sources
- Start Scanning
- Support setup

Internal project team
Effort: 1-2 days

3-4 Workshop



Introduction to the D&M solution & best practice clean-up flow

Introduction to standard organisations communication examples

Project group will try a flow on their own data

Define & plan the organisations roll:

- Test group
- First Wave
- Second Wave
- Etc.

Product owner
Ongoing: 1-2 days a quarter

Roll out



Roll out:

- Test group
- First Wave
- Second Wave
- Etc.

Collect feedback and evaluate

Normal clean-up mail every 3 months

Quarterly status call with Data & More

Duration – approx. 1 month.

Ongoing

Data & More support portal

Hello. How can we help you?

Search for answers



Organisational roll-out

Information & templates & how for the organizational roll out All articles are in different languages, the heading is english



IT Onboarding

The following guides that you will be following when onboarding



Notification Report

How to navigate the notification report and get the most of it.



Cloud data

How to set up service accounts and assign roles for accessing data in mail, onedrive, sharepoint and fileshare



On-Premise Data

How to setup VPN and access On-Premiser data



Enterprise Installation and Setup

Information on Enterprise installation and Setup

Both customers and partners have access to the Data & More support page with relevant information, templates and documents



Got any questions? I'm happy to help.



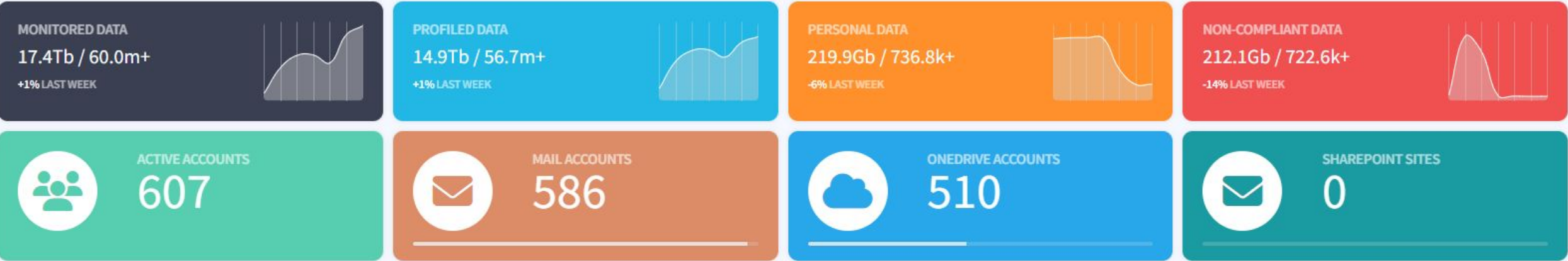


Appendix C

Real world example

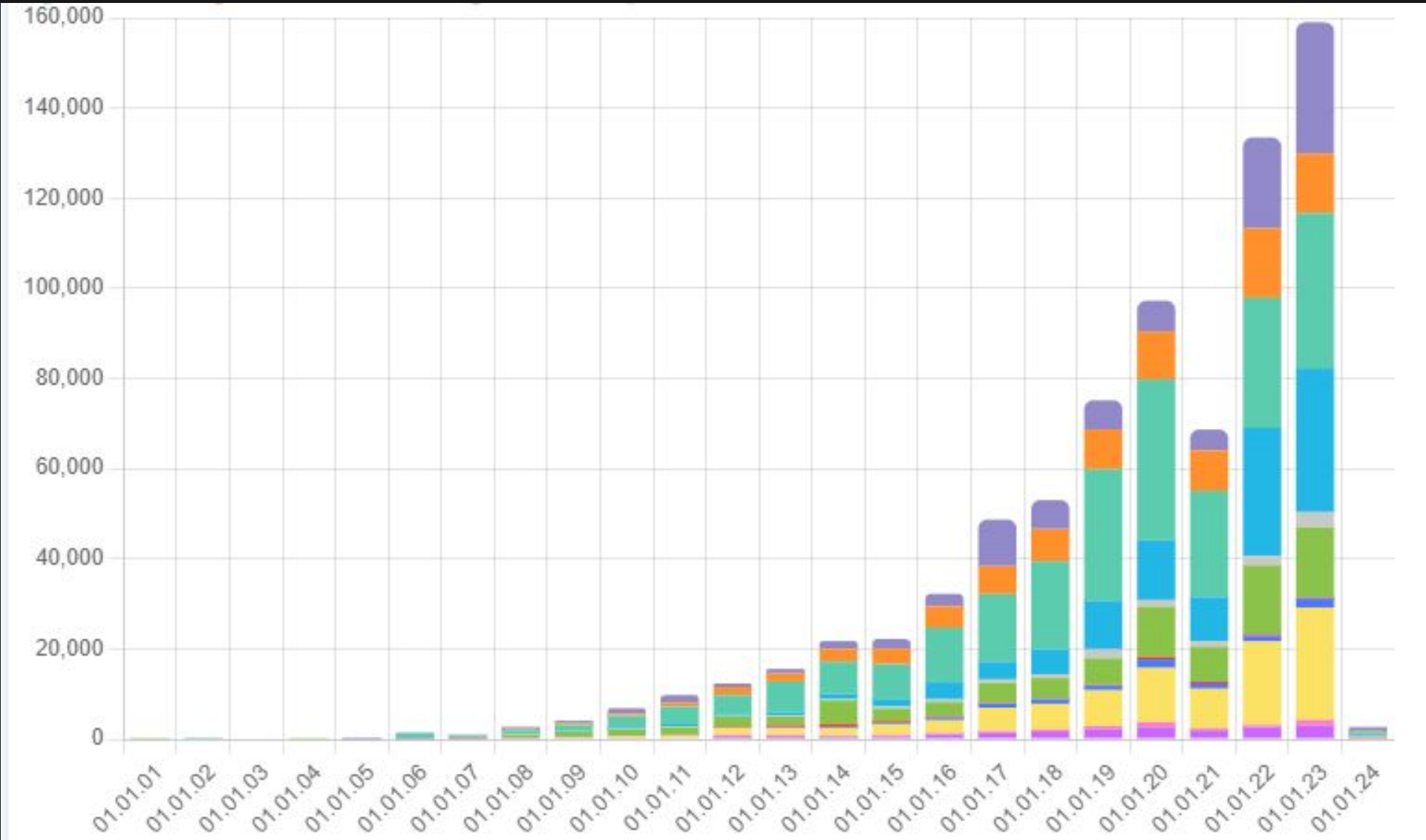
How bad is it

Example: amount of non-compliant data



607 users have 722.600 Non-compliant files

Example: age of non-compliant data is



Appendix D

One pager on why Data More for: Compliance, Security,
Data breach, Copilot and Purview



Compliance

Deletion of "old" personal data is a legal requirement

Applies to all organisations: public, private, NGO and organisations, all legal entities must ensure that sensitive personal data is deleted, when it is no longer a legitimate business purpose.

Responsibility of the controller (Article 24)

"¹[...] the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

²Those measures shall be reviewed and updated where necessary."

<https://gdpr-info.eu/art-24-gdpr/>

Consequences of data privacy non-compliance:

- Fines are up 137% in 2023
- Average fine 1,7 Mio Euro
- Bad PR & loss of reputation
- Possible loss of revenue
- Stricter future auditing from authorities

Finnish SA: Administrative fine of € 856,000 for failing to define storage period of customer data

8 May 2024 Finland



Background information

- > Date of final decision: 6 March 2024
- > National case
- > Legal Reference(s): Article 5 (Principles relating to processing of personal data), Article 25 (Data protection by design and by default)
- > Decision: Administrative fine, Compliance order, Reprimand
- > Key words: Administrative fine, Retention time, Data retention

https://www.edpb.europa.eu/news/national-news/2024/finnish-sa-administrative-fine-eu-856000-failing-define-storage-period_en



Data Breach

Personal sensitive data is the commodity, the more "Illegal" personal sensitive data an organisation has, the bigger the cost, impact, and fines

Personal sensitive data is the target of an attack, it is one of the most vulnerable and valuable types of information for extortion

Communication [...] to the Data Subject (Article 34)

Requirement: If the data breach is likely to result in a high risk to the rights and freedoms of individuals, the company must also communicate the breach to the affected data subjects without undue delay.

https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

Consequences of Data Breach

- 163 € per PII document
- Life threatening business incident
- Average cost of Data Breach 4,4 mio €
- Angry customers, employees etc.
- Risk of extortion
- Stricter audits from Data authorities
- Most likely also a Privacy e.g. GDPR fine in addition to the Data Breach cost

What are hackers stealing?

The report found that nearly half (46%) of all data breaches involve customer personal information like Social Security numbers, emails, phone numbers, and home addresses. Intellectual property, like trade secrets, was stolen in 43% of breaches.

<https://www.ibm.com/reports/data-breach>



Copilot/AI

It is the organisations responsibility to ensure that there is no “illegal” personal sensitive data or oversharing of any data, not Microsoft. If copilot has access to “illegal” personal data or makes overshared data available to more people then necessary, this constitutes a full blown illegal data breach.

Definition of a Data Breach (Article 4)

A "**personal data breach**" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, **unauthorized disclosure of, or access to personal data**"

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679#d1e32-1-1>

Consequences of AI Data Breach

- Data Breach & GDPR Fine
- Many employees can extremely easy get a full overview of other peoples:
 - Personal Sensitive data
 - Logon and passwords info
 - Incriminating behavior

“Because Copilot automatically inherits your existing Microsoft 365 data and security permissions, it makes setup straightforward. It also highlights the importance of having established content management practices and data governance in place before rollout begins”



Security

In almost all organisations users receive different type of login and password information in emails etc. and other critical infrastructure information is sent via e-mail and not deleted. This poses a severe security threat, increasing the risk of Credential Reuse, unauthorized access, Data breaches etc.

Security of Processing (Article 32) in addition (5, 25, 33)

Appropriate Technical and Organizational Measures:

“Storing passwords in unencrypted, free text violates these security measures and can be seen as non-compliance with Article 32”

<https://gdpr.eu/article-32-security-of-processing/>

Consequences security info in free text

- Data Breach cost & GDPR Fine
- Average cost of Data Breach 4,4 mio €
- External hackers access to many different systems
- Hostile take over of multiple systems and users accounts, company and private

In Average there is potentially compromising security information in 1 out of 531 emails (0,19%)

An average organization with 500 users has between 35-40.000 compromising security information in freetext



Purview

Microsoft Purview is a comprehensive set of solutions that can help your organization govern, protect, and manage data, if data can be classified correctly

For Purview to work – it requires a compliant GDPR privacy classification

Microsoft's classifications in Purview represent only a fraction of what is necessary to meet regulations like GDPR. Moreover, many of the classifications provided lack precision, leading to a high rate of false positives and negatives. It is up to the customer to build a compliant privacy classification

Consequences of Purview implementation

It requires the following for Purview to work

- A full mapping of the GDPR privacy classification types in all major languages and countries
- A full mapping of what those types constitute in each major language and country
- Have 5+ person multilanguage full time specialist classification team
- Define & Build & Validate & Maintain these thousands of classification in multiple different languages
- Develop a full end-user data clean-up validation flow
- Develop a custodian mapping system
- Develop exception handling functionality
- Develop full compliance reporting

Appendix E

Pricing

Pricing:

Pricing is based on data sources, and if they are cloud only or also some on prem = hybrid

01. Data Sources:

Only O365 Mail (Cloud)

O365 Mail (Cloud)

On premise & Cloud

02. Select currency

CHOOSE CURRENCY			
☐ DKK ☐ USD	 D&M FOR EXCHANGE ONLINE GET IN TOUCH >	 D&M FOR MICROSOFT 365 GET IN TOUCH >	 D&M FOR HYBRID GET IN TOUCH >
O365 Mail	✓	✓	✓
O365 OneDrive	✗	✓	✓
O365 SharePoint	✗	✓	✓
O365 Teams	✗	✓	✓
Fileshare (on-prem)	✗	✗	✓
Exchange (on-prem)	✗	✗	✓
SharePoint (on-prem)	✗	✗	✓
# of Accounts	Subscription/Month *	Subscription/Month *	Subscription/Month *
0-49	260€	390€	1.775€
50-99	460€	575€	1.775€
100-174	775€	900€	1.775€
175-249	1.075€	1.250€	1.775€
250-499	1.350€	1.475€	2.100€
500-749	1.600€	1.800€	2.500€
750-999	2.000€	2.250€	3.250€
1000-1999	3.400€	3.700€	5.200€
2.000-2.999	4.500€	5.000€	7.000€
3.000-3.999	5.200€	5.800€	8.250€

03. Number of accounts
e.g. 800 accounts = 750-999

4. = Price per month

<https://dataandmore.com/prices/>